Cyberdaders: uniek profiel, unieke aanpak?

Een onderzoek naar kenmerken van en passende interventies voor daders van cybercriminaliteit in enge zin

Eindrapportage – December 2019

Dr. W. van der Wagen[1]

Dr. E.G van 't Zand-Kurtovic[2]

S.R. Matthijsse MSc[1]

Dr. T.F.C. Fischer[1]

Met medewerking van: Sophie Keizer en Nicole Alberts

[1] Erasmus Universiteit Rotterdam, Sectie Criminologie

[2] Universiteit Leiden, Instituut voor Strafrecht en Criminologie

COLOFON

Opdrachtgever

Wetenschappelijk Onderzoek- en Documentatiecentrum (WODC)

Afdeling Externe Betrekkingen (EWB) Ministerie van Justitie en Veiligheid

Koningskade 4

2596 AA Den Haag

Onderzoekers

Dit onderzoek is uitgevoerd door de sectie Criminologie van de Erasmus Universiteit Rotterdam in samenwerking met de Universiteit Leiden. De betrokken onderzoekers waren: Wytske van der Wagen, Elina van ’t Zand, Sifra Matthijsse en Tamar Fischer, met medewerking van Sophie Keizer en Nicole Alberts.

Illustratie voorblad: https://tumblr.com

Samenvatting

Achtergrond en onderzoeksvragen

Er zijn verschillende indicaties dat hacken[3], het uitvoeren van DDoS-aanvallen[4], het verspreiden van ransomware[5] en andere vormen van cybercriminaliteit in enge zin[6] in omvang toenemen onder zowel jeugdigen als volwassenen. De wetenschappelijke kennis over deze dadergroep is tot op heden beperkt, anekdotisch, verouderd en versnipperd. In dit onderzoek is getracht op meer systematische wijze kennis over de kenmerken en profielen van jeugdige en volwassen daders van cybercriminaliteit in enge zin te genereren alsook inzichten te bieden in de vraag wat hierbij passende en effectieve interventies zijn. In dit onderzoek staat de volgende probleemstelling centraal:

"In hoeverre bestaan er verschillen qua profiel(en) van cyberdaders en daders van 'traditionele' criminaliteit, en in hoeverre en op welke wijze dienen (eventuele) verschillen gevolgen te hebben voor de aard van interventies voor cyberdaders?"

Methoden van onderzoek

In dit kwalitatieve onderzoek is gebruik gemaakt van een combinatie van onderzoeksmethoden. Ten eerste zijn twee systematische zoekopdrachten in de literatuur verricht: een gericht op kenmerken van cyberdaders en een gericht op interventies voor cyberdaders. De eerste zoekopdracht leverde 99 bronnen op over kenmerken van daders van cybercriminaliteit in enge zin, al dan niet in vergelijking met traditionele daders. De tweede zoekopdracht leverde 25 bronnen op over interventies gericht op cyberdaders in enge zin. Ten tweede zijn expertinterviews afgenomen (29 individuele interviews, 2 focusgroepen, 1 expertmeeting en 1 roundtable). In totaal zijn 52 experts gesproken, vanuit vrijwel alle samenwerkingspartners uit de veiligheidsketen (politie, Openbaar Ministerie, rechterlijke macht, advocatuur, (jeugd)reclassering, Raad voor de Kinderbescherming, Halt en zorgverleners) evenals experts uit het bedrijfsleven, onderzoekers en freelancers die zich met het thema cybercriminaliteit bezighouden. Ten derde zijn 14 volwassen daders geïnterviewd. Hiervan was het grootste deel veroordeeld voor een of meer cyberdelicten in enge zin (o.a. hacken, DDoS-aanvallen, virtuele diefstal[7]) en een kleiner deel was wel betrokken bij cyberdelicten, maar waren daarvoor niet gepakt. In de meeste gevallen was hacken het primaire delict. De justitiële interventies die de geïnterviewde daders opgelegd hebben gekregen betreffen voornamelijk taakstraffen, maar ook hebben sommige daders een (voorwaardelijke) gevangenisstraf, contactverbod, geldboete, schadevergoeding of elektronische detentie opgelegd gekregen. Vier daders hebben geen justitiële interventie opgelegd gekregen en twee daders waren ten tijde van het interview nog in afwachting van hun strafzaak.

[3] Dit verwijst naar het wederrechtelijk binnendringen in een computersysteem.
[4] Dit verwijst naar verstoren of platleggen van een systeem door middel van overbelasting.
[5] Dit verwijst naar kwaadaardige software (*malware*) die gebruikt kan worden om een systeem 'te gijzelen' c.q. te blokkeren opdat het slachtoffer losgeld moet betalen.
[6] Dit verwijst naar vormen van cybercriminaliteit waarbij ICT zowel het doelwit als het middel is.
[7] Dit verwijst naar het stelen van goederen in een virtueel spel.

Beperkingen van het onderzoek

Het onderzoek kent een aantal beperkingen. Ten eerste kent de gevonden literatuur haar beperkingen. Zo is er relatief veel literatuur gevonden over hackers (zij het wel veel verouderde literatuur en meestal kleine steekproeven), maar weinig over daders die betrokken zijn bij andere vormen van cybercriminaliteit in enge zin zoals DDoS aanvallen en ransomware. Tevens zijn er weinig (effect)studies gevonden waarin de toepassing van traditionele of cyber-gerelateerde interventies op cyberdaders is onderzocht, waardoor er dus weinig systematische kennis over interventies voor handen is. Ten tweede zijn bij de expertinterviews diverse respondenten betrokken die zelf nog maar met enkele cyberdaders ervaring hadden. De antwoorden van deze experts zijn dus bepaald door een klein aantal zaken en verder wellicht medebepaald door verhalen van collega's, beelden uit de media of het maatschappelijke debat. Ten derde vormen de geïnterviewde daders een specifieke groep (volwassen, meerderheid veroordeeld en met hacken als primair delict), waardoor minder focus ligt op andere dadertypen in dit onderzoek. Ten slotte zijn de uitkomsten afhankelijk van zelfrapportage door de daders. Het is mogelijk dat daders niet al hun delictgedrag rapporteerden, recente delicten verzwegen of juist hun delictcarrière 'succesvoller' afschilderden dan ze werkelijk waren.

Bevindingen

DEEL 1 Daderkenmerken

In het eerste deel van het rapport is stilgestaan bij de vraag wat de specifieke kenmerken zijn van cyberdaders en in hoeverre op basis daarvan verschillende daderprofielen te construeren zijn. De kenmerken zijn bovendien vergeleken met kenmerken van traditionele daders waardoor verschillen met deze daders konden worden beschreven. We onderscheiden (offline en online) criminogene (risicofactoren die een bijdrage leveren aan het delictgedrag) en protectieve (beschermende) factoren (factoren die delictgedrag kunnen voorkomen of afremmen). Bij de analyse van de dadergroep is gebruik gemaakt van verschillende algemene criminologische benaderingen zoals de differentiële-associatietheorie[8], neutralisatietechnieken[9] en de rationele keuzetheorie.[10] Ook zijn concepten toegepast die specifiek ontwikkeld zijn om online en technische aspecten van daderschap te duiden zoals het *online disinhibition effect*[11], *digital drift*[12] en *mastery.*[13]

Profielen

Gedurende het onderzoek bleek dat een eenvoudige clustering of profilering op grond van het wel of niet aanwezig zijn van bepaalde kenmerken geen realistisch beeld oplevert. Bij de daders zijn verschillende

[8] Deze theorie veronderstelt dat delinquent gedrag wordt aangeleerd in hechte groepen. Daarbij gaat om zowel technieken om criminaliteit te plegen als normen, waarden en attitudes.
[9] Dit zijn technieken die daders kunnen gebruik om delinquent gedag goed te praten.
[10] Deze benadering gaat er vanuit dat delinquent gedrag voortvloeit uit en begrepen kan worden als een rationele kosten- en batenafweging. Het kan daarbij gaan om zowel materiële (geld) als niet- materiële kosten en baten (roem, plezier).
[11] Dit verwijst naar het wegvallen van remmingen door online anonimiteit.
[12] Dit verwijst naar de wijze waarop het internet zowel technische als sociale *affordances* biedt die bepaalde vormen van delinquentie kunnen intensiveren of daar nieuwe mogelijkheden voor bieden.
[13] Dit verwijst naar de behoefte of drang om de techniek meester te zijn en gaat gepaard met een gevoel van macht en controle.

kenmerken en factoren (persoonlijk en contextueel) en specifieke motivaties (zoals uitdaging zoeken of status verwerven) aanwezig, die in verschillende combinaties en mate voorkomen. Dit leidt vervolgens tot (een bepaalde ontwikkeling in) het delictgedrag (criminele carrière). Om deze reden is de profilering van cyberdaders benaderd door het beschrijven van de impact van verschillende kenmerken en factoren op het delictgedrag, zowel individueel als in hun onderlinge samenhang.

Achtergrondkenmerken

Uit de literatuur is gebleken dat cybercriminaliteit in enge zin relatief vaker wordt gepleegd door jonge autochtone mannen met een redelijk tot goede sociaaleconomische achtergrond. Bij de subgroep financieel georiënteerde daders van cybercriminaliteit in enge zin ligt de leeftijd waarop gestart wordt met het plegen van cybercriminaliteit doorgaans hoger, lijkt vaker sprake te zijn van allochtone daders en zijn er indicaties voor een lagere sociaaleconomische status.

Hoewel het opleidingsniveau bij cyberdaders varieert, lijkt sprake te zijn van een relatief hoger intelligentie- en opleidingsniveau in vergelijking met traditionele daders. Soms maken daders hun opleiding niet af, wat niet automatisch betekent dat zij in laaggeschoold werk terechtkomen. Het werk en de opleiding die cyberdaders doen of hebben gedaan varieert, maar opleidingen en banen in de IT-sector zijn oververtegenwoordigd. In hun vrije tijd houden cyberdaders zich veel bezig met techniek, ICT, gamen en sociale media. Hiernaast hebben ze echter ook een breed scala aan andere hobby's. De thuissituatie (o.a. de rol van gezinsproblematiek) varieert sterk. Er blijkt vaak een gebrek aan ouderlijk toezicht op het online gedrag van cyberdaders te zijn, zowel in gezinnen met als zonder gezinsproblematiek. Dit beperkte toezicht wordt mede veroorzaakt door gebrekkige kennis van ouders[14] van het internet en de online wereld.

Tot slot kunnen de cyberdaders gekenmerkt worden als intelligent met vaker dan bij traditionele daders de aanwezigheid van kenmerken uit een autismespectrumstoornis (ASS) en een sterk probleemoplossend vermogen. Tevens suggereren de bevindingen dat er een tweedeling waarneembaar is tussen de cyberdaders die een lagere zelfcontrole ervaren en impulsief zijn en daders die juist lange termijn doelen stellen en perfectionistisch zijn. Sommige daders kunnen volgens de literatuur en de experts gekenmerkt worden als introvert of sociaal onhandig, maar een ander deel (waar veel van de door ons geïnterviewde cyberdaders zichzelf onder scharen) lijkt voldoende sociaal vaardig. Waar de meeste cyberdaders online een sociaal netwerk hebben opgebouwd lijkt het offline netwerk relatief kleiner te zijn en in mindere mate van invloed te zijn op het delictgedrag.

Drijfveren en beleving

Uit het onderzoek komt naar voren dat diverse drijfveren een rol spelen bij cyberdaders. Ook is gebleken dat daders meerdere motivaties hebben en dat motivaties over de tijd heen kunnen veranderen.

De drijfveren nieuwsgierigheid, leergierigheid en (mentale) uitdaging spelen voornamelijk een rol bij jeugdige cyberdaders. Deze motieven zijn niet per definitie kwaadaardig. Deze jongeren willen de *ins and outs* van systemen leren en ontdekken hoe ver ze kunnen gaan met de techniek. Anders dan bij de meeste traditionele vormen van criminaliteit is het leren een doel of drijfveer op zichzelf en niet slechts een middel of instrument om de delicten te kunnen plegen.

[14] Mogelijk is de IT-kennis van ouders wel afhankelijk van hun leeftijd. Dit is in het huidige onderzoek niet specifiek onderzocht.

Andere motieven die naar voren komen zijn de kick, spanning, plezier, verveling, verzameldrang (naar informatie) en macht. Deze drijfveren kunnen ook bij traditionele criminaliteit spelen, maar bij cybercriminaliteit is er een meer nadrukkelijke samenhang met online vaardigheden en techniek.

Erkenning, status, peer respect en bewijsdrang komen als belangrijke motieven naar voren bij jeugdige daders. Deze jongeren willen bewijzen wat ze kunnen om respect of roem te verwerven. Het verschil met traditionele misdaad is dat de focus sterker ligt op de technische vaardigheden, werkwijze en prestatie (je 'kunnen').

Financiële motieven lijken in mindere mate een rol te spelen bij jeugdige (individuele) daders. In sommige gevallen kan geld wel op een later moment in de criminele carrière een rol gaan spelen. Dit is ook afhankelijk van de activiteiten die zij ontplooien. Het financiële motief lijkt vooral voor te komen bij (volwassen) daders die actief zijn in de context van fraude en georganiseerde cybercriminaliteit. In een deel van de gevallen gaat het dan om daders die de overstap hebben gemaakt van traditionele (offline) fraude naar cybercriminaliteit.

Aanvullend kan cybercriminaliteit (voornamelijk hacken of het uitvoeren van DDoS-aanvallen) gepleegd worden uit boosheid of om wraak te nemen op vrienden, familie, ex-werkgevers of ex-geliefden waar offline een conflict mee is ontstaan. Hierbij lijkt het voornamelijk te gaan om volwassen traditionele daders die een nieuw middel hebben ontdekt om hun frustratie te uiten. Ook zijn er daders die uit ideologische motieven handelen. Laatstgenoemde twee clusters van motieven zijn relatief onderbelicht gebleven in dit onderzoek.

Percepties strafbaarheid, pakkans en schade door gepleegde delicten

Als het gaat om de perceptie ten aanzien van strafbaarheid lijkt sprake te zijn van een glijdende schaal. Aan de ene kant van de schaal bevinden zich (veelal jonge) daders die zich niet of nauwelijks bewust zijn van de strafbaarheid en aan de andere kant daders die dat wel zijn en bijvoorbeeld via fora goed op de hoogte zijn van de straffen die ze riskeren.

De gebrekkige perceptie van strafbaarheid, die aanwezig is bij een deel van de daders, komt onder andere voort uit de afwezigheid van toezicht in de online wereld, de onzichtbaarheid van de aangerichte schade en - voor een deel van de daders - de aanwezigheid van drijfveren die in aanleg niet kwaadaardig zijn (nieuwsgierigheid, mentale uitdaging, erkenning van talenten). Binnen deze laatste categorie vallen ook de delicten waarbij beveiligingsproblemen worden aangetoond, maar onduidelijkheid bestaat over de juridische grenzen en de kaders van *responsible disclosure*.[15] Daarmee is de beperkte perceptie van strafbaarheid een belangrijkere criminogene factor bij cyberdaders dan bij traditionele daders. Met het voortgaan van de carrière neemt het besef van de strafbaarheid bij daders toe, maar wordt dit volgens experts deels weer teniet gedaan door de zeer beperkte zichtbaarheid van politie en justitie als het gaat om online criminaliteit.

De pakkans schatten daders over het algemeen erg laag in vanwege beperkte politiecapaciteit en de ruime mogelijkheden voor anonimisering. De bevindingen laten tevens zien dat daders het risico om gepakt te worden over tijd, naarmate men vaker ongezien wegkomt, steeds lager gaan inschatten.

[15] *Responsible Disclosure* (RD) betreft het "binnen de ICT-wereld (...) op een verantwoorde wijze en in gezamenlijkheid tussen melder en organisatie openbaar maken van ICT-kwetsbaarheden op basis van een door organisaties hiervoor vastgesteld beleid voor responsible disclosure" (Nationaal Cyber Security Centrum, 2013, p. 5).

Ten aanzien van de perceptie van de schade is naar voren gekomen dat daders, vooral jonge daders, de omvang en ernst van de schade als gering inschatten alsook de schade bagatelliseren of ontkennen (neutralisatie). Hoewel ontkenning van het slachtoffer of de aangerichte schade ook bij daders van traditionele criminaliteit voorkomt, wordt dit online versterkt door de afstand tot slachtoffer, de hyperrealiteit waarin het gedrag tot stand komt (het voelt als spel), de normalisering die ontstaat door gamen (waar het routine en normaal is om elkaar te DDoSsen of te hacken) en door het gemak waarmee bepaalde delicten (in hoge frequentie) gepleegd kunnen worden. Tevens zorgt de online omgeving voor minder remmingen vanwege afwezigheid van het oordeel van anderen of andere gevreesde consequenties. Door de online anonimiteit van daders en slachtoffers vindt dus een andere evaluatie van het gedrag door de dader plaats, dan wanneer de interactie offline zou zijn (ook wel *online disinhibition effect* genoemd). Bij oudere daders lijkt het bagatelliseren van de schade een minder grote rol te spelen. Zij erkennen de schade maar de drijfveren die zij hebben voor het gedrag (financieel, wraak, ideologisch, etc.) zijn voor hen belangrijk genoeg om de carrière voort te zetten.

Criminele carrières

Bij het in kaart brengen van criminele carrières van daders is gekeken naar factoren die een rol spelen bij het ontstaan (de initiatie), de ontwikkeling van de carrière en wat daders (los van een interventie) doet stoppen.

Als het gaat om de initiatie, zien we dat net als bij traditionele criminaliteit factoren zoals de *maturity gap* (de discrepantie tussen biologische en maatschappelijke volwassenheid), de invloed van delinquente *peers* (vrienden of leeftijdsgenoten) en bepaalde drijfveren (bijvoorbeeld geld, uitdaging of spanning) een rol spelen. Daarnaast zijn er factoren naar voren gekomen die specifiek een rol spelen bij de initiatie bij cybercriminaliteit zoals de interesse voor/affiniteit met ICT, gamen, veel tijd op fora spenderen en/of gemakkelijke toegang tot (kant-en klare) tools. In het kader van de ontwikkeling en rijping van de criminele carrière is uitgegaan van vier fasen die daders deels of allemaal doorlopen: 1) affectie voor computers (fase waarin interesse voor computers/IT ontstaat), 2) nieuwsgierige exploratie (fase waarin een interesse in hacken ontstaat), 3) illegale excursie (fase waarin illegale activiteiten worden geëxploreerd en ook een start gemaakt wordt met het plegen hiervan) en 4) criminele exploitatie (fase waarin stelselmatig delicten worden gepleegd). Gebleken is dat er veel variatie is met betrekking tot welke fase(n) door de daders word(t)(en) doorlopen. Dit kan variëren van daders die niet verder komen dan ‘nieuwsgierige exploratie’ en (doorgaans volwassen opportunistische) daders die gelijk in de ‘criminele exploitatie’ fase terecht komen tot daders die alle fasen doorlopen.

Ook bij daders die dezelfde fasen doorlopen, bestaat variatie als het gaat om hoe de ontwikkeling van het delictgedrag eruit ziet en welke factoren daarop van invloed zijn. Deze variaties hangen grotendeels samen met factoren die een rol spelen bij de initiatie alsook met de motieven, vaardigheden en mate van professionalisering. Tegelijkertijd spelen andere processen een rol als het gaat om het verloop van de criminele carrière, waaronder veranderingen in morele percepties (ofwel richting pro-crimineel ofwel richting pro-sociaal gedrag) en veranderingen in motieven (bijvoorbeeld van erkenning naar financieel).

Bij *desistance* (het stoppen met criminaliteit) zien we eveneens dat diverse factoren een rol spelen. Net als bij traditionele daders hebben volwassenwording en het krijgen van werk en een wederhelft invloed op het stoppen. Verondersteld wordt hierbij wel, voornamelijk door de experts, dat

cyberdaders relatief meer kansen hebben op een (goede) baan vanwege de maatschappelijk behoefte aan digitaal talent. Ook laten de bevindingen zien dat er door de tijd heen, wat ook weer samenhangt met leeftijd en sociale bindingen, andere kosten en baten een rol kunnen gaan spelen. Daarbij zien we ook terug dat de motieven die aanvankelijk ervoor zorgden dat de daders deze delicten gingen plegen (bijvoorbeeld kick, uitdaging en spanning) er ook weer voor zorgen dat ze er mee stoppen. Over tijd nemen deze aspecten af of vallen helemaal weg. In het kader van stoppen wordt ook gewezen op factoren die *desistance* bemoeilijken. Naast het hebben van een strafblad wordt in dit kader gewezen op het feit dat daders helemaal kunnen opgaan in de online (delinquente) wereld, zowel in termen van status en identiteit als (het snelle) geld, waardoor er nog te veel (materiële en immateriële) baten zijn om niet te stoppen.

DEEL 2 Interventies

In het tweede deel van het onderzoek is gefocust op de vraag in hoeverre bestaande interventies[16] voldoende aansluiten bij de (in deel 1) geschetste kenmerken en factoren. Aangezien interventies voor specifiek cyberdaders schaars zijn en er bovendien weinig (evaluatie)onderzoek is gedaan naar zowel traditionele als alternatieve interventies voor cyberdaders, zijn de bevindingen vooral gebaseerd op verwachtingen over de effectiviteit die uit de literatuur en de interviews konden worden afgeleid.

In de analyse van potentieel effectieve interventies is in de eerste plaats gekeken naar interventies gericht op afschrikking en situationele criminaliteitspreventie, die direct ingrijpen op de perceptie van de kosten-baten verhouding bij het plegen van cybercriminaliteit (rationele keuzebenadering). In de tweede plaats zijn interventies besproken die ingrijpen op de bestaande criminogene en protectieve factoren voor het plegen van cybercriminaliteit bij het individu en de verschillende contexten waarin het individu verkeert (op basis van *What Works* en de *desistance* benadering[17]). Hierbij wordt een onderscheid gemaakt tussen *risk-based* interventies, die ingrijpen op kenmerken die van invloed zijn op het delictgedrag (criminogene factoren/behoeften) en *strength-based* interventies, die meer gefocust zijn op aangrijpingspunten om het proces van de ontwikkeling van pro-sociaal gedrag en een pro-sociale identiteit te ondersteunen. Deels betreffen dit aangrijpingspunten voor het opheffen van risicofactoren, maar vooral wordt aangesloten bij protectieve factoren (*strengths*), zoals het ontwikkelen van talent, waarmee kansen voor de toekomst en daarmee perspectief en hoop wordt geboden. De *responsiviteit* van daders voor de geboden interventie is bij beide benaderingen een belangrijke thema.

[16] We hanteren in het rapport een vrij ruime definitie van het begrip interventie. Alternatieven zoals hackwedstrijden noemen we in dit rapport 'interventie' omdat ze ingezet kunnen worden om gedragsbeïnvloeding te bewerkstelligen.

[17] *Risk-based* interventies sluiten nauwgezet aan bij inzichten uit de *What Works* benadering, waarbij de nadruk ligt op de behandeling van criminogene factoren. *Strength-based* interventies vinden vooral aansluiting bij theorieën over desistance. Echter, de benaderingen en hun inzichten over effectieve interventies overlappen elkaar ook gedeeltelijk. In het huidige onderzoek zetten we ze dan ook niet tegen over elkaar, maar beschouwen we als complementair. Tevens moet benadrukt worden dat sommige interventies zowel *risk-based* als *strength-based* elementen hebben.

Interventies die aansluiten bij de theorie van afschrikking en situationele criminaliteitspreventie

Volgens de rationele keuzebenadering zouden interventies effectief zijn als ze ofwel de kosten voor het plegen van een delict verhogen ofwel de baten verlagen. Situationele preventiestrategieën[18] (zoals *warning banners*[19] en het verstoren van digitale markten) kunnen een rol spelen bij het verhogen van het risico en de noodzakelijke inspanningen voor criminaliteit. Van alle beschreven interventies is verstoring (maatregelen gericht op het verstoren van het criminele uitvoeringsproces) de interventie die het meest direct ingrijpt op de inspanningen die geleverd moeten worden om delicten te plegen en daarmee op de kosten van het delict. Subgroepen voor wie deze interventie mogelijk effectief zijn, zijn daders met financiële drijfveren in alle fasen van hun loopbaan en daders (ongeacht hun drijfveren) die hun delicten plegen met behulp van gekochte tools.

Andere interventies die zich richten op verhoging van de gepercipieerde kosten, zijn interventies gericht op bewustwording van de risico's die het delict voor de dader meebrengt (zoals de kans op straf) of van de aangerichte schade (bewustzijn over deze schade kan gewetensvragen oproepen). Of dergelijke interventies effectief zijn, hangt af van de mate waarin de daders open staan voor de informatie die in de interventies wordt overgedragen (responsiviteit). Verondersteld kan worden dat deze interventies niet effectief zijn voor meer ervaren daders en daders die er drijfveren op na houden waarbij de strafbaarheid een onderdeel is van de opbrengsten (bijvoorbeeld spanning of status).

Belangrijk is dat bij deze interventies door experts ook steeds gewezen wordt op mogelijk averechtse effecten, zoals het genereren van nog meer spanning (die juist ten grondslag ligt aan plegen van de delicten) en het nemen van extra afschermingsmaatregelen door de daders. Daarentegen kan door de zichtbaarheid (van politie/justitie) die bewerkstelligd wordt met interventies gericht op bewustwording van de risico's, ook het gevoel van onaantastbaarheid verdwijnen en een aangepaste kosten-batenuitkomst ontstaan, wat hen mogelijk doet afzien van cyberdelicten.

Uit de bevindingen kan verder worden opgemaakt dat ten aanzien van de zekerheid, ernst en snelheid waarmee straf volgt op cybercriminaliteit (voorwaarden voor een afschrikwekkende werking) nog veel winst valt te behalen. Zowel de gepercipieerde als de daadwerkelijke pakkans wordt als zeer laag beschouwd door experts evenals daders. Daarnaast lijken volgens de experts de doorlooptijden van opsporing, vervolging en berechting bij cyberzaken langer te zijn dan bij 'traditionele' zaken, hetgeen onder meer te maken heeft met het feit dat het opsporingsonderzoek en ook het leveren van het bewijs complexer is.

Het antwoord op de vraag hoe 'zwaar' de straffen dienen te zijn om voldoende afschrikwekkend effect te sorteren, hangt volgens experts vooral af van de motivatie van de dader, waarbij een onderscheid wordt gemaakt tussen daders met een financieel motief en daders die jong, *first offender* en door nieuwsgierigheid gedreven zijn. Voor de laatstgenoemde groep daders zou het opgepakt worden of zelfs de dreiging daarmee middels een waarschuwingsgesprek met de politie (*knock and talk*) vaak al voldoende afschrikwekkend kunnen werken en bewustwording van strafbaarheid en schade teweegbrengen. Indien een interventie lange tijd nadat het delict gepleegd is alsnog wordt opgelegd (en de jongere mogelijk alweer veel verder is in zijn of haar ontwikkeling en/of al gestopt is) kan de interventie, indien geen rekening wordt gehouden met resocialiserende aspecten (zoals het geval is bij hoge boetes of lange gevangenisstraffen), voor deze groep een averechts effect sorteren. Tegelijkertijd zou volgens de

[18] Het gaat om preventieve strategieën die gericht zijn op het wegnemen van de gelegenheid om criminaliteit te plegen en dus de risicoperceptie (en kosten) van de dader vergroten.

[19] Dit zijn digitale waarschuwingsberichten om te voorkomen dat iemand online delictgedrag vertoont.

literatuur en experts een voorbeeld gesteld moeten worden naar de samenleving toe door bij ernstige cyberzaken waar ondanks de lage pakkans toch een arrestatie en veroordeling volgt, ook een zware straf op te leggen. Daarvan zou volgens de respondenten een generaal preventief effect uitgaan (signaalfunctie).

Interventies die aansluiten bij de *What Works* en de *desistance* benadering

Risk-based interventies

Over (de effectiviteit van) de inzet van interventies gericht op de criminogene behoeften van cyberdaders (*risk*-based interventies) is in de literatuur en bij experts nog weinig bekend. Een belangrijke constatering hierbij is dat er nog nauwelijks sprake is van gevalideerde risicotaxatie bij deze groep daders. In de eerste plaats bleek dat er nog maar beperkt zicht is op hoe de criminogene factoren bij cyberdaders precies gemeten moeten worden (voorbeelden waren de kwaliteit van de ouderlijke supervisie en de wijze waarop persoonlijke en psychologische kenmerken gerelateerd kunnen worden aan delictgedrag in de online context). Daardoor lijken bestaande diagnose-instrumenten nog onvoldoende gevalideerd ten aanzien van de criminogene en protectieve factoren waarop interventies specifiek bij cyberdaders ingezet moeten worden. Daarnaast geven verschillende experts aan dat er van (tijdige) risicotaxatie met de noodzakelijke verdiepende analyse door deskundigen bij deze dadergroep nog onvoldoende sprake is. Hiervoor lijkt een juiste 'routering' in het afdoeningsproces noodzakelijk.

Als het gaat om de vraag welke interventies effectief zouden kunnen zijn voor cyberdaders, wordt door experts veelal verwezen naar bestaande interventies voor traditionele daders. Deze zijn gericht op diverse leefgebieden zoals het verbeteren van de relatie met ouders, het aanleren van sociale vaardigheden, het aanpakken van een pro-criminele houding en het werken aan schulden of verslaving. Deze interventies zouden effectief kunnen zijn voor het aanpakken van de betreffende criminogene factor bij daders van verschillende leeftijden en in verschillende fasen van de criminele loopbaan mits motivatie voor verandering aanwezig is of kan worden gecreëerd. De verwachting is echter dat cyberdaders in het algemeen onvoldoende responsief zullen zijn voor (de meeste van) deze interventies omdat deze geen of te weinig rekening houden met de online context waarin de delicten plaatsvinden (waarin schade minder zichtbaar is en het slachtoffer erg 'abstract'). Om daar meer rekening mee te houden, wordt door experts verwacht dat een methode als *mentaliseren*, wat inleven in een ander inhoudt, zinvol kan zijn. Ook verwachten experts, ondanks zeer beperkte ervaring hiermee, positieve effecten van contact met het slachtoffer door middel van herstelbemiddeling.

De enige specifiek op cyberdaders gerichte interventies die gevonden zijn, zijn het opleggen van restricties rondom computer- en internetgebruik en de inzet van *serious gaming*. Bij dit laatste worden jongeren op een spelende manier goede en slechte manieren van hacken geleerd en worden ze tegelijkertijd aan het denken gezet hierover. Dergelijke interventies kunnen onder meer zorgen voor het afsluiten van contact met online criminele *peers* (een belangrijke criminogene factor). Een dergelijke afsluiting is echter complex te bewerkstelligen en zal altijd tijdelijk zijn. Deze interventie moet dus gezien worden als een interventie die een momentum schept voor andere interventies die op de langere termijn *desistance* in gang kunnen zetten (door bijvoorbeeld het ombuigen van de pro-criminele houding en het aanreiken van alternatieven). De inzet van *serious gaming* is potentieel effectief voor jonge, niet-kwaadwillende daders die op deze manier spelenderwijs bewust worden gemaakt van goede en slechte

aspecten van het hacken. Dit is daarmee een relatief lichte interventie die bij kan dragen aan kennis over ethiek en bewustwording bij jonge hackers. Hoewel geen negatieve effecten kunnen worden verwacht van deze interventie, blijft het nog de vraag of de effecten die gegenereerd worden in een spelsetting ook in 'real life' effect hebben. Daar staat weer tegenover dat *serious gaming* plaatsvindt in een context van begeleiding en er naar alle waarschijnlijkheid over ethische grenzen wordt gesproken. Bij dit laatste resteert de vraag in hoeverre men vatbaar (responsief) is voor deze informatie en of hun morele kompas daadwerkelijk wordt bijgestuurd. Meer onderzoek is nodig om antwoord te kunnen geven op deze vragen.

Strength-based interventies

Behalve voor interventies gericht op het verminderen van criminogene behoeften, is in de literatuur en onder experts ook aandacht voor *strength-based* interventies, interventies die vooral gericht zijn op het versterken van de pro-sociale identiteit. Meer dan bij daders van traditionele criminaliteit zijn bij een deel van de daders van cybercriminaliteit in engere zin talenten (technische vaardigheden) aanwezig die veel waarde hebben voor de samenleving mits ze op een pro-sociale manier worden ingezet (ethisch hacken). Interventies kunnen hierbij aansluiten door perspectieven te bieden van wat zij met deze vaardigheden zouden kunnen bereiken op de arbeidsmarkt. Door experts in dit kader veelgenoemde preventieve interventies zijn cyberwerkplaatsen[20] en hackwedstrijden.[21] Deze interventies zijn gericht op het vergroten van IT-vaardigheden en het aanleren van ethisch hacken. Door dergelijke interventies krijgen jongeren tevens erkenning, leren zij gelijkgestemden kennen (die net als zij veel interesse in IT hebben) en wordt gebouwd aan (zowel technische als sociale) vaardigheden en toekomstperspectief. Een andere vorm van een *strength-based* interventie(onderdeel) is begeleiding door rolmodellen.[22] Uit zowel de literatuur als de expertinterviews komt naar voren dat dit een belangrijk element is bij het opbouwen van een nieuwe prosociale identiteit en relaties. Rolmodellen kunnen ook een signaalfunctie hebben, omdat eventueel grensoverschrijdend gedrag opgemerkt en gecorrigeerd kan worden.

Een specifiek op cyberdaders gerichte (reactieve) interventie is de recent ontwikkelde Hack_Right interventie, die zich onder meer richt op het versterken van talent en het ethisch leren hacken door middel van een leerwerkplek bij een IT-bedrijf, waarbij ervaren hackers als coaches (rolmodellen) worden ingezet. De interventie lijkt goed aan te sluiten bij de *desistance* benadering, omdat wordt beoogd jonge cyberdaders op weg te helpen naar een pro-sociale identiteit en rol in de samenleving. Hoewel de interventie formeel nog door de Erkenningscommissie Justitiële Interventies[23] moet worden erkend, zijn experts erg verwachtingsvol over wat dit voor de doelgroep (jong, *first offender*, technisch vaardig, geen ernstig delict, schuld bekend en gemotiveerd) kan betekenen. Ook zijn er enkele kritische geluiden, bijvoorbeeld waar het gaat om de vraag of een dergelijke interventie strafbaar gedrag juist niet beloont. Bezien vanuit de theorie van afschrikking, genereert een dergelijke interventie mogelijk onvoldoende specifieke en wellicht ook generale afschrikking.

Bij de inzet van *strength-based* interventies is het uiteraard van belang dat de juiste doelgroepen worden geselecteerd, waarbij de drijfveren voor het delictgedrag een belangrijk criterium lijken te vormen. Alleen werken aan het vergroten van de IT-vaardigheden en het bieden van een netwerk of carrièrekansen zonder dat gewerkt wordt aan het moreel besef en het ombuigen van een eventuele pro-

[20] Een plek waar IT-vaardige jongeren terecht kunnen om bijvoorbeeld workshops te volgen of aan IT-projectjes te werken

[21] Dit zijn doorgaans door private partijen gesponsorde hackwedstrijden waarbij hackers op verzoek systemen hacken

[22] In dit geval gaat het om mensen uit de hackerswereld (bijvoorbeeld ethische hackers) die een voorbeeldfunctie en/of mentorrol vervullen.

[23] Voor meer informatie over deze commissie en de werkwijze, zie: https://www.nji.nl/nl/Databank/Databank-Effectieve-Jeugdinterventies/Deelcommissie-Justitiele-interventies

criminele houding, kan immers tot meer cybercriminaliteit leiden. Indien de verschillende onderdelen in combinatie terugkomen in de interventie, bieden *strength-based* interventies niet alleen kansen aan cyberdaders, maar zouden ze mogelijk ook tot een afname van toekomstig daderschap kunnen leiden en daarmee tot een positieve uitkomst voor de samenleving.

Conclusies en aanbevelingen

In dit onderzoek is een analyse gemaakt van de (unieke) kenmerken van cyberdaders en de mate waarin beschikbare interventies aansluiten bij deze kenmerken. Het onderzoek laat zien dat we met alles behalve een homogene groep daders te maken hebben. Er is veel variatie te zien, zowel wat betreft drijfveren als criminogene en protectieve factoren voor het plegen van cybercriminaliteit. In meer algemene zin kan geconcludeerd worden dat een aantal criminogene factoren zowel bij traditionele daders als bij cyberdaders een rol spelen, zoals gezinsproblematiek, bagatellisering van ernst en schade van het gepleegde delict evenals bepaalde motieven (kick, plezier en geld). Echter, door de online omgeving en (technische) aard van de delicten kunnen zij anders tot uiting komen. Tevens hebben we kenmerken aangetroffen die relatief vaker voor lijken te komen bij cyberdaders dan bij traditionele daders of vrij uniek zijn voor deze dadergroep. Hier gaat het bijvoorbeeld om persoonlijkheids- of psychologische kenmerken die bijdragen aan de noodzakelijke talenten voor het tot stand komen van de delicten (nieuwsgierigheid, leergierigheid, zelfcontrole, perfectionisme, behoefte aan erkenning en bewijsdrang ten aanzien van technische vaardigheden) of om persoonlijkheids- of psychologische kenmerken die offline sociale interactie bemoeilijken (zoals introversie, kenmerken van een autismespectrumstoornis en sociale onhandigheid).

Naar aanleiding van onze bevindingen kunnen een drietal aanbevelingen worden gedaan met betrekking tot de wijze waarop interventies voor cyberdaders vormgegeven moeten worden.

In de eerste plaats is het van belang dat er *meer* en meer *toegesnede*n verdiepingsdiagnostiek plaatsvindt ten behoeve van beslissingen over (strafrechtelijke) interventies voor cyberdaders. Nu de diversiteit onder cyberdaders groot blijkt, is een op maat gesneden aanpak van belang en daartoe moeten de criminogene en protectieve kenmerken en de wijze waarop deze het delictgedrag in de online omgeving beïnvloeden in kaart worden gebracht. De huidige instrumenten lijken nog onvoldoende in staat om deze specifieke cyberdader gerelateerde kenmerken te meten. Naast criminogene behoeften is daarbij ook specifiek aandacht nodig voor responsiviteit voor interventies (leerstijlen en motivaties) van cyberdaders die in een online omgeving hun delicten plegen. Voor cyberdaders lijkt het aangewezen dat specifieke aanvulling op bestaande diagnose-instrumenten beschikbaar komt.

In de tweede plaats lijken interventies waarin bewustwording, mentaliseren (inleven in de ander), moreel redeneren (in combinatie met ethisch hacken) en het aanbieden van kansen gecombineerd worden veel potentie te hebben om effectief te zijn voor met name jonge technisch vaardige daders. Echter, deze interventies blijken ook ongewenste effecten op te kunnen leveren, omdat ze daders onbedoeld op ideeën kunnen brengen of de status van cyberdaders bij hun *peers* kunnen verhogen. Het is dus belangrijk om van deze interventies zowel de bedoelde als de onbedoelde effecten goed te onderzoeken en duidelijke doelgroepen te beschrijven voor wie de interventies potentieel effectief zijn effectief zijn.

In de derde plaats bleek dat voor zowel jongere als oudere daders in verschillende fasen van de criminele loopbaan, maar met andere drijfveren dan nieuwsgierigheid en het zoeken van mentale

uitdaging, traditionele interventies potentieel geschikt zijn. Dit betreft de interventies die zich richten op specifieke criminogene factoren (zoals verslaving, gebrek aan sociale vaardigheden of ondersteunende relaties). Deze interventies houden echter nog geen rekening met de responsiviteit van cyberdaders in de online context waardoor de effectiviteit voor deze doelgroep waarschijnlijk tegenvalt. Onze laatste aanbeveling is dan ook om na te gaan welke aanpassingen er in deze bestaande interventies nodig zijn om aan te sluiten bij de responsiviteit van cyberdaders.